RECEIVED
2014 AUG 12 PM 1:41
PAUL FERGUSON, CLERK
ARLINGTON CIRCUIT COURT

VIRGINIA:

IN THE CIRCUIT COURT FOR THE COUNTY OF ARLINGTON

MAXIENT, LLC, a Virginia limited liability company, with an address of record of P.O. Box 7224, Charlottesville, Virginia 22906,	§	
Plaintiff,	§	
v.	§	**Civil Action No.** 14-1822
SYMPLICITY CORPORATION, a Delaware corporation, with its principal place of business located at 1560 Wilson Blvd., Arlington, Virginia 22209	§	**Jury Trial Demanded**
Serve: Registered Agent Ariel Manuel Friedler 1560 Wilson Blvd., Suite 550, Arlington, Virginia 22209,	§	
ARIEL MANUEL FRIEDLER, an individual resident of the Commonwealth of Virginia, residing at 1881 N. Nash St., unit 1506, Arlington, Virginia 22209,	§	
ALOK KUMAR DHIR, an individual resident of the State of Maryland, residing at 8610 Hartsdale Ave., Bethesda, Maryland 20817,	§	
and	§	
MATTHEW KELLEY, an individual resident of the State of Connecticut, residing at 14 Valley Ln., Fairfield, Connecticut 06825,	§	
Defendants.	§	

COMPLAINT

Plaintiff Maxient, LLC ("Maxient"), by and through its undersigned counsel of record, submits its Complaint against Symplicity Corporation ("Symplicity"), Ariel Manuel Friedler

("Friedler"), Alok Kumar Dhir ("Dhir"), and Matthew Kelley ("Kelley") (all collectively, "Defendants"), and alleges as follows:

I. NATURE OF THE ACTION

1. This is a lawsuit concerning Defendants' hacking and misappropriation of Plaintiff Maxient's trade secrets, and proprietary and confidential information.

2. Plaintiff seeks recourse from Defendant Symplicity and its top officials who engaged in multiple and deliberate campaigns to successfully and unlawfully access Plaintiff Maxient's computer network in order to steal and misappropriate Maxient's trade secrets and proprietary and confidential information.

II. THE PARTIES

3. Plaintiff Maxient is a Virginia limited liability company with its principal place of business located in Charlottesville, Virginia, with its address of record at P.O. Box 7224, Charlottesville, Virginia, 22906.

4. Defendant Symplicity is a Delaware corporation with its principal place of business located at 1560 Wilson Blvd., Arlington, Virginia 22209.

5. At all relevant times, Defendant Friedler was the President, Chief Executive Officer ("CEO") and founder of Symplicity, who resides at 1881 N. Nash St., unit 1506, Arlington, Virginia 22209.

6. At all relevant times, Defendant Dhir was the Chief Technology Officer ("CTO") of Symplicity, who resides at 8610 Hartsdale Ave., Bethesda, Maryland 20817.

7. At all relevant times, Defendant Kelley was the Director of Sales for Symplicity, who resides at 14 Valley Ln., Fairfield, Connecticut 06825.

III. JURISDICTION AND VENUE

8. This Court has jurisdiction over this action and the named parties pursuant to Virginia Code § 8.01-328.1 as this action arose under the laws of the Commonwealth of Virginia and the injury occurred in Arlington County. Symplicity's principal place of business is in Arlington County and it regularly transacts and/or contracts to supply services in Virginia and has appointed a registered agent for service of process in Virginia.

9. This Court is the proper venue pursuant to Va. Code § 8.01-262(B) because some or all of the causes that gave rise to this action occurred in Arlington County.

IV. STATEMENT OF FACTS

10. Maxient is a Charlottesville, Virginia-based company that, since its inception in 2003, has been engaged in the business of providing a web-based software called *Conduct Manager* to institutions of higher education for managing the processes and records related to student conduct (i.e., student conduct record management, or "SCRM").

11. Maxient has approximately ten (10) employees.

12. Symplicity is an Arlington, Virginia-based corporation and is a direct competitor to Maxient in the market of higher education SCRM, where Symplicity offers a competing product called at times "JAMS" or "Advocate."

13. Symplicity is a multi-million dollar company with approximately 150 employees whose clients include the White House and members of Congress.

14. Maxient's method of providing SCRM follows the Software-as-a-Service ("SaaS") model and involves creating unique instances of its software for each client institution. Maxient provides its distributed solution through protected servers that are accessible to its subscribers over a secure Internet connection. Maxient's design features are critical means by

which it competes with Symplicity products and these design features are the lifeblood of the business.

15. Upon information and belief, Symplicity follows a substantially similar model in its offerings.

16. Maxient's software system is itself a proprietary invention, utilizing unique formulas, techniques, processes, functions, features and methods, all constituting trade secrets which provide Maxient's customers a valuable solution over competing software solutions.

17. Among the many measures taken to protect Maxient's trade secrets and proprietary and confidential information, Maxient strictly limits access to its client systems to authorized users only, requires its employees and clients to agree to confidentiality provisions in their respective agreements with Maxient, and appropriately marks both the software's internal screens as well as any protected accompanying documentation with conspicuous indicators of their confidential nature.

18. Many of the facts alleged in this Complaint are sourced from signed admissions by Defendants Friedler and Dhir in connection with their respective criminal prosecutions for conduct in part described in this Complaint. *See* **Exhibits A & B**.

19. By January 2010, Symplicity had begun to lose client institutions in the SCRM market to Maxient. By September 2010, this trend continued such that Symplicity's CEO (Friedler) wrote to Symplicity's CTO (Dhir) and Symplicity's Director of Sales (Kelley), in addition to other Symplicity employees, the following regarding their competing Advocate product: "...we are bleeding advocate alok -- we have lost close to a dozen this year." *See* **Exhibit A at pg. 4**.

20. On or about September 13, 2010, Symplicity's CEO requested another Symplicity

employee to provide email addresses and encrypted passwords of individual users at one of Symplicity's former client institutions that had switched to Maxient. This institution is referred to in Friedler's and Dhir's criminal filings ("the Criminal Filings") as "University No. 1." Symplicity's CEO explicitly told Symplicity's CTO: "... want to see if we can use old client who used us to get into maxient -- ill do it from somewhere else... there are some online tools that give u reverse if they are common words." *Id.*

21. Based on information and belief, Symplicity maintained its former clients' personal information which included, at least a user name and encrypted password.

22. Symplicity's CTO decrypted passwords of employees at another former Symplicity client institution that had switched to Maxient, "University No. 2," and provided those to Symplicity's CEO. Symplicity's CEO also requested Symplicity's CTO to decrypt passwords used by employees of another former client institution, "University No. 3," telling Symplicity's CTO, "... desperate times calls for desperate measures." *Id.* Symplicity's CTO complied, including providing Symplicity's CEO with the specific login credentials of an employee of University No. 3, identified in the Criminal Filings as "Employee B."

23. On or about September 13, 2010, Symplicity's CEO and CTO tested the use of The Onion Router Project, better known as "TOR," a system intended to enable online anonymity and used to mask the origin of activities undertaken online. Based on information and belief, TOR can be used for the concealment of illegal activities.

24. That evening, using TOR, Symplicity's CEO, falsely posing as and using the login credentials of Employee B of former client University No. 3, successfully accessed Maxient's protected servers. While deceptively logged in as Employee B of University No. 3, Symplicity's CEO reviewed Maxient's trade secrets and confidential and proprietary product design and

manuals, and copied-and-pasted key proprietary and confidential information into a 110-page document and saved it on Symplicity's computer as "maxient.docx" ("the Maxient Document"). The Maxient Document contained, *inter alia*, detailed information about Maxient's new and key features, planned upgrades, layout of the software, and key screen shots. The information improperly obtained by Symplicity's CEO included information that was obviously confidential, proprietary and trade secret information of Maxient. Indeed, various screen shots copied by Symplicity explicitly stated: "The information contained on these pages is privileged and confidential information intended solely for the individual or entity who has accessed it for official purposes and by lawful means. Any dissemination, distribution, or copy of this communication is strictly prohibited." *Id.*

25. On or about September 15, 2010, Symplicity's CEO and Symplicity's Director of Sales discussed which stolen Maxient features to add to Symplicity's SCRM product. Later that day, Symplicity's CEO cautioned Symplicity's Director of Sales to avoid referring to the unauthorized access outside of communications with specific Symplicity employees, including Dhir, the CTO who had participated and was already involved. Symplicity's Director of Sales agreed.

26. On or about January 10, 2011, following the migration of clients from Symplicity to Maxient, Symplicity's CEO and Symplicity's CTO discussed ways of obtaining additional usernames and decrypted passwords of employees at University No. 3.

27. On or about August 11, 2011, Symplicity's CTO provided Symplicity's CEO with additional usernames, encrypted passwords, and decrypted passwords used by University No. 3 and another institution, "University No. 4." About four days later, Symplicity's CTO provided Symplicity's CEO with additional usernames and passwords for employees at University No. 1.

28. On or about August 17, 2011, Symplicity's CEO successfully accessed Maxient's protected servers by improperly posing as and using the login credentials of an individual staff member of University No. 1, identified in the Criminal Filings as "Employee C." Symplicity's CEO also attempted to further access the system with credentials of another employee of University No 1, identified in the Criminal Filings as "Employee A." Following Symplicity's CEO's unauthorized access of August 17, 2011, Symplicity's Director of Sales, using Maxient's confidential information, sent an email to other Symplicity employees containing ideas and talking points for how Symplicity could distinguish Symplicity's SCRM product from Maxient's.

29. Maxient detected both the successful and attempted unauthorized accesses of University No. 1 on August 17, 2011 and notified the FBI immediately. These instances marked the first time that Maxient was aware of any unauthorized accesses into any protected Maxient system. However, Maxient did not know the source of the unauthorized intrusions or the extent of the harm because the intruders masked their Internet origins using TOR.

30. On information and belief, in a series of emails entitled "Maxient features to add," Symplicity's CEO directed employees to use the stolen confidential, proprietary and trade secret information about Maxient's design features to develop similar features in Symplicity. *See* **Exhibit C at pg. 2.**[1]

31. On information and belief, in commenting on the implementation of Maxient features in Symplicity products, Symplicity's CEO wrote, "this is one of the only features maxient had we did not… whole reason i wanted it built was for schools who may demo them

[1] Attached as Exhibit C is the Position of the United States with Respect to the Sentencing of Friedler, submitted by the U.S. Department of Justice in connection with Friedler's sentencing hearing.

and say how come symp doesnt have it… how can we ensure that everyone knows we have this capabilitiy [sic]?" *See id.* Symplicity used these features to unfairly compete against Maxient in the SCRM market in part by depriving them of their status as a sole source provider for these features.

32. On or about August 19, 2011, FBI Special Agent in Charge, Michael Morehart, requested that Maxient not disclose the potential security breach and not notify Maxient customers. Agent Morehart stated that notification could impede the criminal investigation.

33. On or about March 19, 2012, the FBI executed a search of Symplicity's premises in furtherance of its investigation into the matter and seized Symplicity laptops and hard drives (among other evidence). The FBI then proceeded to conduct a computer forensic examination of the seized computer data.

34. In the course of the FBI's forensic examination, the FBI found the Maxient Document stored on Symplicity's computers. The FBI believed that this document and the proprietary and confidential information and trade secrets contained therein resulted from Defendants' unlawful intrusion into Maxient's secure network and Conduct Manager.

35. In approximately August 2013, the FBI presented for the first time the Maxient Document to Aaron Hark, a Maxient co-owner and Chief Software Architect. Hark confirmed that the document contained stolen information concerning Maxient's software and that the information included Maxient's trade secrets and proprietary and confidential information, which was not otherwise available to the public or unauthorized third-parties.

36. During the FBI's investigation, FBI agents and the U.S. Attorney's office requested that Maxient refrain from seeking civil recourse or otherwise divulging any information related to the facts of the investigation until the FBI had completed the investigation

and the U.S. Department of Justice had completed its prosecution.

37. As a result of the FBI's investigation, in May 2014, the United States Government charged Symplicity's CEO, Friedler, and Symplicity's CTO, Dhir, with federal computer hacking crimes. *See* **Exhibit D & E** (referencing Friedler and Dhir's plea agreement). Specifically, Defendants Friedler and Dhir were charged with violating the Computer Fraud and Abuse Act (18 U.S.C § 1030) for unlawful access to a protected computer network and conspiracy to commit same. *See Id.*

38. On May 21, 2014, Symplicity's CEO pleaded guilty to conspiring to hack into Maxient's secure system for the purpose of improving Symplicity's software development and sales strategy. *See* **Exhibit D**. On June 4, 2014, Symplicity's CTO pleaded guilty to conspiring to hack into Maxient's secure system for the purpose of improving Symplicity's software development and sales strategy. *See* **Exhibit E**.

39. The extent of Defendants' actions was further revealed in an April 11, 2014, signed statement by Friedler in connection with his guilty plea. *See* **Exhibit A.** In that statement, Friedler admits that he conspired with other Symplicity employees to knowingly and intentionally access Maxient's protected computers in order to obtain information for the purpose of seeking commercial advantage and private financial gain. *Id.*

40. The statement of facts signed by Friedler admittedly contain the facts to support Defendant Friedler's guilty plea and are not wholly inclusive of all facts relating to the harm inflicted upon Maxient. *Id.*

41. As a result of Defendants' wrongful actions, Plaintiff Maxient has been and continues to be injured.

42. Based on information and belief, Defendants stole Plaintiff Maxient's trade

secrets and proprietary and confidential intellectual information for use in Symplicity's competing SCRM solution.

43. Based on information and belief, Defendants used Maxient's trade secrets and proprietary and confidential information in order to unfairly compete against Maxient.

44. Based on information and belief, Defendants used Maxient's trade secrets and proprietary and confidential information by incorporating them into Symplicity's own competing SCRM program.

45. Based on information and belief, Symplicity used this information to unfairly compete with Maxient in the same marketplace.

46. As a result of Defendants' wrongful actions, the value of Maxient's trade secrets and proprietary and confidential information have become diminished and Maxient has lost revenue to which it would otherwise be entitled.

47. In a press release, United States Department of Justice officials stated that Defendants' "actions caused significant harm to their competitors and ultimately gave Symplicity an unfair business advantage." (http://www.justice.gov/opa/pr/2014/May/14-crm-543.html).

48. Defendants Friedler, Dhir, and Kelley were, in all matters alleged herein, acting as agents of Defendant Symplicity, within the scope of their duties and in furtherance of Symplicity's interests and to benefit Symplicity. The acts complained of were not of rogue employees, but Symplicity's top officials. *See* **Exhibits A-C.**

49. Because Plaintiff Maxient's causes of actions arise out of the same set of facts that led to the prosecution and conviction of Defendants Friedler and Dhir, Plaintiff is entitled to a suspension of applicable statutes of limitation under Virginia Code § 8.01-229(K). In the

alternative, Defendants' concealed their actions which Plaintiff was only able to discover with the assistance from federal authorities.

50. Plaintiffs have suffered substantial monetary damages as a result of Defendants' conduct.

51. In addition to the monetary damages, the Plaintiffs have suffered and continue to suffer irreparable harm to which they do not have an adequate remedy at law.

52. Due to Defendants' wrongful conduct, which is without justification or excuse, as described in this Complaint, Plaintiff is likely to succeed on the merits of its claims.

COUNT ONE

MISAPPROPRIATION OF TRADE SECRETS - VIRGINIA CODE § 59.1-336[0] ET SEQ AGAINST ALL DEFENDANTS

53. Plaintiff restates and realleges each of the allegations set forth above and incorporates them herein.

54. Plaintiff Maxient maintains trade secrets and proprietary and confidential information including, but not limited to, formulas, patterns, compilations, programs, devices, methods, techniques, and processes, that constitute Maxient's trade secrets.

55. Maxient's trade secrets derive actual and potential independent economic value from their confidential nature and give Maxient a competitive advantage.

56. Maxient's trade secrets are not generally known to, and are not readily ascertainable by proper means by, other persons who can obtain economic value from their disclosure.

57. Maxient's trade secrets are the subject of efforts that are reasonable under the circumstances to maintain their secrecy and Maxient has pursued an active course of conduct to protect its trade secrets.

58. Plaintiff Maxient's protected and secured computer network and servers contain trade secrets including, but not limited to, its proprietary and confidential software solution called "Conduct Manager".

59. Defendants stole Maxient's trade secrets and proprietary and confidential information and knew or had reason to know that the trade secrets and proprietary and confidential information were acquired by improper means.

60. Defendants stole knowledge and information on Maxient's Conduct Manager solution by gaining electronic unauthorized access to Maxient's protected network and Conduct Manager.

61. Defendants disclosed and/or used a trade secret and proprietary and confidential information of Maxient without express or implied consent by Maxient, by improper means to acquire knowledge of the trade secret and/or at the time of disclosure or use, Defendants knew or had reason to know that knowledge of the trade secret was derived from or through a person who had utilized improper means to acquire it. *See* Va. Code § 59.1-336.

62. On multiple occasions, Defendants used a computer and a computer network to access Maxient's protected network and servers to copy, steal and misappropriate Maxient's trade secrets and proprietary and confidential information, including Conduct Manager. Defendants knew that they had utilized improper means to acquire Maxient's trade secrets and proprietary and confidential information.

63. As an actual and proximate result of Defendants' conduct, Maxient has suffered substantial damages in an amount to be proven at trial.

64. Plaintiff Maxient's damages include actual loss and the unjust enrichment caused by the misappropriation. Additionally, Maxient is entitled to lost profits and/or a reasonable

royalty for Defendants' unauthorized disclosure and/or use of Maxient's trade secrets and proprietary and confidential information.

65. As a result of Defendants' conduct, Maxient has been damaged in the approximate amount of $5,000,000.

66. Defendants' actions were willful and malicious, and Plaintiff Maxient also is entitled to punitive damages in the amount of $350,000.

67. As a result of Defendants' conduct, Maxient is entitled to reasonable attorney's fees under Virginia Code § 59.1-338.1.

68. As a result of Defendants' conduct, Plaintiff also requests that this Court enjoin the Defendants from engaging in acts of misappropriation and continuing to use and/or benefit in any way from Plaintiff's stolen trade secrets, proprietary information or confidential information in accordance with Virginia Code § 59.1-337.

COUNT TWO

COMPUTER FRAUD - VIRGINIA CODE § 18.2-152.3 AGAINST SYMPLICITY AND FRIEDLER

69. Plaintiff restates and realleges each of the allegations set forth above and incorporates them herein.

70. Symplicity and Symplicity's CEO used a computer and a computer network without authorization with the intent to obtain Maxient's property and services by false pretenses and converted the property of another. *See* Va. Code § 18.2-152.3.

71. Symplicity and Symplicity's CEO intended to and did access and use Maxient's secured computers and secured network without authority by posing as Maxient's subscribers with the intent to obtain Maxient's property and services. Further, Symplicity and Symplicity's

CEO converted Maxient's trade secrets, proprietary and confidential information, and intellectual property by fraudulently accessing Maxient's computers and secured network.

72. As a result of such conduct, Maxient has been damaged in the approximate amount of $5,000,000.

73. Symplicity and Symplicity's CEO's actions were willful and malicious, and as such Maxient is entitled punitive damages in the amount of $350,000.

74. As a result of Defendants' conduct, Plaintiff also requests that this Court enjoin the Defendants from engaging in acts of computer fraud against Maxient.

COUNT THREE

COMPUTER TRESPASS - VIRGINIA CODE §18.2-152.4 AGAINST SYMPLICITY AND FRIEDLER

75. Plaintiff restates and realleges each of the allegations set forth above and incorporates them herein.

76. With malicious intent Symplicity and Symplicity's CEO used a computer and a computer network without authorization to make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network. *See* Va. Code § 18.2-152.4.

77. With malicious intent Symplicity and Symplicity's CEO used a computer and a computer network without authorization with the intent to make or cause to be made an unauthorized copy of computer data residing in Maxient's secured computers and secured network.

78. As a result of such conduct, Maxient has been damaged in the approximate amount of $5,000,000.

79. Symplicity and Symplicity's CEO's actions were willful and malicious, and as such Maxient is entitled punitive damages in the amount of $350,000.

80. As a result of Defendants' conduct, Plaintiff also requests that this Court enjoin the Defendants from engaging in acts of computer trespass against Maxient.

COUNT FOUR

ENCRYPTION USED IN CRIMINAL ACTIVITY - VIRGINIA CODE §18.2-152.15 AGAINST SYMPLICITY, FRIEDLER, and DHIR

81. Defendants Symplicity, Symplicity's CEO, and Symplicity's CTO willfully used encryption to further criminal activity, including, but not limited to, violating 18 U.S.C. §§ 371,1030(a)(2)(C) and (c)(2)(B)(i).

82. Defendants Symplicity, Symplicity's CEO, and Symplicity's CTO enciphered unintelligible data, such as encrypted passwords, into intelligible and decrypted form.

83. As a result of such conduct, Maxient has been damaged in the approximate amount of $5,000,000.

84. Symplicity, Symplicity's CEO, and Symplicity's CTO's actions were willful and malicious, and as such Maxient is entitled punitive damages in the amount of $350,000.

85. As a result of Defendants' conduct, Plaintiff also requests that this Court enjoin the Defendants from engaging in acts of password encryption in criminal activity against Maxient.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Maxient respectfully requests that the Court:

A. Enter judgment in favor of Maxient and against the Defendants on all counts, jointly and severally, for $5,000,000 in compensatory damages or such other amount as may be proven at trial;

B. Award Plaintiff punitive damages in the amount of $1,400,000;

C. Award Plaintiff its costs and disbursements;

D. Award Plaintiff reasonable attorneys' fees under Virginia Code § 59.1-338.1;

E. Award Plaintiff pre-judgment and post-judgment interest to the maximum extent provided under the law;

F. Award Plaintiff such further and additional relief as is deemed appropriate by this Court; and

G. Permanently enjoin Defendants, their agents, servants, and employees, and all those in privity with Defendants or in active concert and participation with Defendants, from engaging in acts of misappropriation, computer fraud, computer trespass, password encryption in criminal activity, and/or use and/or benefit from Plaintiff's stolen and misappropriated trade secrets and proprietary and confidential information.

JURY DEMAND

Plaintiff hereby demands a jury on all issues so triable.

Dated: August 12, 2014

Respectfully submitted,

PLAINTIFF MAXIENT, LLC
By Counsel

Bernard J. DiMuro, Esq. (VSB #18784)
Stephen L. Neal, Esq. (VSB # 87064)
Taylor S. Chapman, Esq. (VSB # 81968)
Counsel for Plaintiff Maxient, LLC
DIMUROGINSBERG, PC
1101 King Street, Suite 610
Alexandria, Virginia 23314
Telephone: (703) 684-4333
Facsimile: (703) 548-3181
E-mail: bdimuro@dimuro.com;
sneal@dimuro.com;
tchapman@dimuro.com

FILED
IN OPEN COURT
MAY 21 2014

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA
v.
ARIEL MANUEL FRIEDLER,
Defendant

Criminal No. 1:14-cr-181

STATEMENT OF FACTS

The United States and the defendant, Ariel Manuel Friedler, agree that had this matter proceeded to trial, the United States would have proven the following facts in the Eastern District of Virginia and elsewhere beyond a reasonable doubt:

1. Symplicity Corporation ("Symplicity") was a corporation headquartered in Arlington, Virginia, in the Eastern District of Virginia. Symplicity offered higher education software products for colleges and universities, federal government systems development for communications management products used by the United States government, including the White House and members of Congress, and secure managed hosting. Symplicity also sold a Student Conduct Records Management ("SCRM") system allowing colleges and universities to track student disciplinary records. Its SCRM product was called "Advocate" or "JAMS."

2. Defendant ARIEL MANUEL FRIEDLER was the Chief Executive Officer and president of Symplicity.

3. A.D. was Symplicity's Chief Technology Officer responsible for software development and systems administration.

4. M.K. was Symplicity's Director of Higher Education Product Sales.

ALL-STATE LEGAL®
EXHIBIT
A

5. Maxient LLC ("Maxient") was headquartered in Charlottesville, Virginia, and also competed against Symplicity in the SCRM business. Maxient's product was called "Conduct Manager."

6. Company A was headquartered in Texas, and competed against Symplicity in the SCRM business.

7. Companies providing SCRM systems derive their competitive edge from the design and features of the system, which they consider proprietary and confidential. As a result, they require clients or potential clients to sign agreements with non-disclosure provisions, and frequently file open records requests to learn more about their competitors.

8. From on or about October 17, 2007, and continuing thereafter until on or about October 27, 2011, in the Eastern District of Virginia and elsewhere, the defendant, ARIEL MANUEL FRIEDLER, together with A.D. and M.K., each knowingly and intentionally conspired and agreed together and with each other, and with others, to commit an offense against the United States, that is, to knowingly and intentionally access a computer without authorization, and thereby obtain information from a protected computer, and the offense was committed for purposes of commercial advantage and private financial gain, in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(i).

9. Defendant ARIEL MANUEL FRIEDLER led the conspiracy, organized the intrusions, recruited employees to decrypt encrypted passwords, and used anonymizing software in preparation for intrusions. After accessing sensitive and valuable business information from Symplicity's competitors, FRIEDLER copied, saved, and shared this information with co-conspirators and other employees to inform Symplicity's software development and sales strategy.

10. On or about October 17, 2007, defendant ARIEL MANUEL FRIEDLER gained access to the protected computer systems of Company A without authorization to obtain confidential and proprietary business information from a competitor. Specifically defendant FRIEDLER, without authorization, accessed and copied Company A's confidential and proprietary business information related to the company's client names and information on features into a comprehensive spreadsheet (the "Company A Spreadsheet").

11. Also on or about October 17, 2007, defendant ARIEL MANUEL FRIEDLER sent multiple emails to CW-1 containing a list of Company A's current clients, a list of potential clients that had asked Company A for prices, and the Company A Spreadsheet. FRIEDLER then instructed CW-1, "for [Company A] client list who are also symp customers please send a persaonlzied [sic] email, ccing career center and also telling them we know they are a [Company A] client and we can do a lot more for them."

12. From on or about January 22, 2010 through on or about January 23, 2010, Defendant ARIEL MANUEL FRIEDLER and A.D. exchanged the following messages:

FRIEDLER:	Do u have tor working?
A.D.:	For?
FRIEDLER:	I can't get firefox to not show proxy error when I turn tor on. Was wondering if problem with snow
A.D.:	But all other browsers are fine? That's bizarre. Maybe try clearing cache etc? Ff works fine for me on all my snow machines - 2 havkintosh and 1 MacBook.
FRIEDLER:	sorry -- i meant when using TOR..trying to get into a competitors shit

TOR is a free software tool that allows users to hide their IP address and use the Internet anonymously.

13. On or about January 24, 2010, defendant ARIEL MANUEL FRIEDLER unsuccessfully attempted to log in to Maxient's servers twice without authorization using the login credentials for "Employee A" of "University No. 1."

14. Between at least on or about May 28, 2010 to at least on or about September 11, 2010, Symplicity continued to lose customers to Maxient on the SCRM product line. For example, on or about September 8, 2010, after Maxient won another bid, defendant ARIEL MANUEL FRIEDLER emailed company employees, including A.D. and M.K. that "we need to make advocate a website look and feel that is the point and why we lost [a university client] to maxient today. they said maxient feels like a website and for users that use it a few times a year that is what they are seeking.... we are bleeding advocate alok -- we have lost close to a dozen this year."

15. On or about September 13, 2010, after losing another client to Maxient, defendant ARIEL MANUEL FRIEDLER asked a Symplicity employee for email addresses and the encrypted passwords of a former customer, "University No. 1." Defendant FRIEDLER told A.D.: "want to see if we can use old client who used us to get into maxient -- ill do it from somewhere else... there are some online tools that give u reverse if they are common words."

16. A.D. then used a reverse-lookup website to decrypt passwords for employees of a former client, "University No. 2," and forwarded them to defendant ARIEL MANUEL FRIEDLER, stating: "Holy crap dude – the shit works."

17. Upon receiving the passwords from A.D., defendant ARIEL MANUEL FRIEDLER stated: "u just saved me a ton of time -- can u give me emails that went with this and give me same shit for [University No. 3] desperate times calls for desperate measures."

18. A.D. then emailed to defendant ARIEL MANUEL FRIEDLER a chart of email addresses of employees of former client "University No. 3," the encrypted passwords, and various passwords A.D. had been able to decrypt, including the password for "Employee B."

19. Later that evening, defendant ARIEL MANUEL FRIEDLER and A.D. had the following exchange:

FRIEDLER:	what ip lookup do u get for ip 208.53.142.37[?]
A.D.:	Some weird tor address - guessing that's w the onion routing thing on
FRIEDLER:	cool -- so masked

20. Defendant ARIEL MANUEL FRIEDLER then logged into Maxient's servers using login credentials for "Employee B" from "University No. 3."

21. While logged into Maxient's servers as "Employee B," defendant ARIEL MANUEL FRIEDLER reviewed Maxient's confidential and proprietary product design and manuals, and copied-and-pasted key proprietary and confidential information into a 110-page document and saved it as maxient.docx (the "Maxient Document") on a computer. The Maxient Document contained detailed information about Maxient's new and key features, planned upgrades, layout of the software, and key screen shots. Various screen shots explicitly provided that, "The information contained on these pages is privileged and confidential information intended solely for the individual or entity who has accessed it for official purposes and by lawful means. Any dissemination, distribution, or copy of this communication is strictly prohibited."

22. Two days after the unauthorized access, on or about September 15, 2010, defendant ARIEL MANUEL FRIEDLER and M.K. discussed which features to add to their SCRM product, in an email with the subject line "Maxient features to add."

23. Later that day, defendant ARIEL MANUEL FRIEDLER and M.K. discussed Maxient in an online chat session, during which defendant ARIEL MANUEL FRIEDLER instructed M.K. not to reveal the unauthorized access: "hey until dust settles for me doent [sic] say anythign [sic] ab out seeing competitors shit to anyone but alok or brian which know not worth it in a month or two sure." M.K. responded "ok."

24. After losing several more SCRM clients to Maxient, on or about January 10, 2011, defendant ARIEL MANUEL FRIEDLER and A.D. engaged in the following exchange:

FRIEDLER:	hey – remember that those reverse ahshes [sic] u did a while ago =- i dont want to login again, but deleting that db and want to have just in case do u have it and can u resend
A.D.:	im not entirely sure what we're talking about - the super h@ckery?
FRIEDLER:	y
A.D.:	did i email it?
FRIEDLER:	.uy
A.D.:	then i'd have it - what was the rough date range
FRIEDLER:	oy search for [Employee B] that should pull it up
A.D.:	n
FRIEDLER:	[University No. 3] date range then sept 7-13

Defendant ARIEL MANUEL FRIEDLER and A.D. then discussed how to decrypt additional passwords of former clients, and A.D. sent to defendant ARIEL MANUEL FRIEDLER the chart containing the usernames and decrypted passwords of employees at former client "University No. 3."

25. On or about August 11, 2011, A.D. emailed defendant ARIEL MANUEL FRIEDLER a spreadsheet containing the usernames, encrypted passwords, and decrypted passwords of four former Symplicity clients, including those of "University No. 3" and "University No. 4."

26. On or about August 15, 2011, A.D. emailed to defendant ARIEL MANUEL FRIEDLER the usernames and decrypted passwords for employees of former client, "University No. 1."

27. On or about August 17, 2011, A.F. logged into the Maxient server using the login credentials of "Employee C," an employee at Symplicity's former client "University No. 1." Defendant ARIEL MANUEL FRIEDLER also attempted to login using the username and password for "Employee A," also an employee of Symplicity's former client "University No. 1."

28. A few hours after defendant ARIEL MANUEL FRIEDLER accessed Maxient's systems without authorization on or about August 17, 2011, M.K. sent an email containing ideas and talking points for how to distinguish the Symplicity SCRM product from Maxient's.

29. The statement of facts includes those facts necessary to support the defendant's guilty plea. It does not include each and every fact known to the defendant or to the government and it is not intended to be a full enumeration of all of the facts surrounding the defendant's case.

30. The actions of the defendant, as recounted above, were in all respects knowing and intentional, and were not committed by mistake, accident or other innocent reason.

Dana J. Boente
Acting United States Attorney

By: _____
Alexander T.H. Nguyen
Assistant United States Attorney

Peter V. Roman
Trial Attorney, U.S. Department of Justice
Computer Crime & Intellectual Property Section

Defendant's Signature: After consulting with my attorney, I hereby stipulate that the above Statement of Facts is true and accurate and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.

Date: April 10, 2014

Ariel Manuel Friedler
Defendant

Defense Counsel Signature: I am Ariel Manuel Friedler's attorney. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is an informed and voluntary one.

Date: April 10, 2014

David W. O'Brien, Esq.
Stephen M. Byers, Esq.
Kenneth L. Wainstein, Esq.
Adam S. Lurie, Esq.
Counsel for the Defendant

FILED
IN OPEN COURT
JUN 4 2014
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

ALOK KUMAR DHIR,

Defendant

Criminal No. 1:14-cr-182

STATEMENT OF FACTS

The United States and the defendant, Alok Kumar Dhir, agree that had this matter proceeded to trial, the United States would have proven the following facts in the Eastern District of Virginia and elsewhere beyond a reasonable doubt:

1. Symplicity Corporation ("Symplicity") was a corporation headquartered in Arlington, Virginia, in the Eastern District of Virginia. Symplicity offered higher education software products for colleges and universities, federal government systems development for communications management products used by the United States government, including the White House and members of Congress, and secure managed hosting. Symplicity also sold a Student Conduct Records Management ("SCRM") system allowing colleges and universities to track student disciplinary records. Its SCRM product was called "Advocate" or "JAMS."

2. A.F. was the Chief Executive Officer and president of Symplicity.

3. Defendant ALOK KUMAR DHIR was Symplicity's Chief Technology Officer responsible for software development and systems administration.

4. M.K. was Symplicity's Director of Higher Education Product Sales.

EXHIBIT
B
ALL-STATE LEGAL®

5. Maxient LLC ("Maxient") was headquartered in Charlottesville, Virginia, and also competed against Symplicity in the SCRM business. Maxient's product was called "Conduct Manager."

6. Companies providing SCRM systems derive their competitive edge from the design and features of the system, which they consider proprietary and confidential. As a result, they require clients or potential clients to sign agreements with non-disclosure provisions, and frequently file Freedom of Information Act requests to learn more about their competitors.

7. From on or about October 17, 2007, and continuing thereafter until on or about October 27, 2011, in the Eastern District of Virginia and elsewhere, the defendant, ALOK KUMAR DHIR, together with A.F. and M.K., each knowingly and intentionally conspired and agreed together and with each other, and with others, to commit an offense against the United States, that is, to knowingly and intentionally access a computer without authorization, and thereby obtain information from a protected computer, and the offense was committed for purposes of commercial advantage and private financial gain, in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(i).

8. From on or about January 22, 2010 through on or about January 23, 2010, A.F. and ALOK KUMAR DHIR exchanged the following messages:

A.F.:	Do u have tor working?
DHIR:	For?
A.F.:	I can't get firefox to not show proxy error when I turn tor on. Was wondering if problem with snow
DHIR:	But all other browsers are fine? That's bizarre. Maybe try clearing cache etc? Ff works fine for me on all my snow machines - 2 havkintosh and 1 MacBook.
A.F.:	sorry -- i meant when using TOR..trying to get into a competitors shit

TOR is a free software tool that allows users to hide their IP address and use the Internet anonymously.

9. On or about January 24, 2010, A.F. unsuccessfully attempted to log in to Maxient's servers twice without authorization using the login credentials for "Employee A" of "University No. 1."

10. Between at least on or about May 28, 2010 to at least on or about September 11, 2010, Symplicity continued to lose customers to Maxient on the SCRM product line. For example, on or about September 8, 2010, after Maxient won another bid, A.F. emailed company employees, including defendant ALOK KUMAR DHIR and M.K. that "we need to make advocate a website look and feel that is the point and why we lost [a university client] to maxient today. they said maxient feels like a website and for users that use it a few times a year that is what they are seeking.... we are bleeding advocate alok -- we have lost close to a dozen this year."

11. On or about September 13, 2010, after losing another client to Maxient, A.F. asked a Symplicity employee for email addresses and the encrypted passwords of a former customer, "University No. 1." A.F. told defendant ALOK KUMAR DHIR: "want to see if we can use old client who used us to get into maxient -- ill do it from somewhere else... there are some online tools that give u reverse if they are common words."

12. Defendant ALOK KUMAR DHIR then used a reverse-lookup website to decrypt passwords for employees of a former client, "University No. 2," and forwarded them to A.F., stating: "Holy crap dude – the shit works."

13. Upon receiving the passwords from defendant ALOK KUMAR DHIR, A.F. stated: "u just saved me a ton of time -- can u give me emails that went with this and give me same shit for [University No. 3] desperate times calls for desperate measures."

14. Defendant ALOK KUMAR DHIR then emailed to A.F. a chart of email addresses of employees of former client "University No. 3," the encrypted passwords, and various passwords DHIR had been able to decrypt, including the password for "Employee B."

15. Later that evening, A.F. and defendant ALOK KUMAR DHIR had the following exchange:

A.F.:	what ip lookup do u get for ip 208.53.142.37[?]
DHIR:	Some weird tor address - guessing that's w the onion routing thing on
A.F.:	cool -- so masked

16. A.F. then logged into Maxient's servers using login credentials for "Employee B" from "University No. 3."

17. While logged into Maxient's servers as "Employee B," A.F. reviewed Maxient's confidential and proprietary product design and manuals, and copied-and-pasted key proprietary and confidential information into a 110-page document and saved it as maxient.docx (the "Maxient Document") on a computer. The Maxient Document contained detailed information about Maxient's new and key features, planned upgrades, layout of the software, and key screen shots. Various screen shots explicitly provided that, "The information contained on these pages is privileged and confidential information intended solely for the individual or entity who has accessed it for official purposes and by lawful means. Any dissemination, distribution, or copy of this communication is strictly prohibited."

18. Two days after the unauthorized access, on or about September 15, 2010, A.F. and M.K. discussed which features to add to their SCRM product, in an email with the subject line "Maxient features to add."

19. Later that day, A.F. and M.K. discussed Maxient in an online chat session, during which A.F. instructed M.K. not to reveal the unauthorized access: "hey until dust settles for me doent [sic] say anythign [sic] ab out seeing competitors shit to anyone but alok or brian which know not worth it in a month or two sure." M.K. responded "ok."

20. After losing several more SCRM clients to Maxient, on or about January 10, 2011, A.F. and defendant ALOK KUMAR DHIR engaged in the following exchange:

A.F. :	hey – remember that those reverse ahshes [sic] u did a while ago =- i dont want to login again, but deleting that db and want to have just in case do u have it and can u resend
DHIR:	im not entirely sure what we're talking about - the super h@ckery?
A.F.:	y
DHIR:	did i email it?
A.F.:	.uy
DHIR:	then i'd have it - what was the rough date range
A.F.:	oy search for [Employee B] that should pull it up
DHIR:	n
A.F.:	[University No. 3] date range then sept 7-13

A.F. and DHIR then discussed how to decrypt additional passwords of former clients, and DHIR sent to A.F. the chart containing the usernames and decrypted passwords of employees at former client "University No. 3."

21. On or about August 11, 2011, defendant ALOK KUMAR DHIR emailed A.F. a spreadsheet containing the usernames, encrypted passwords, and decrypted passwords of four former Symplicity clients, including those of "University No. 4."

22. Also on or about August 11, 2011, defendant ALOK KUMAR DHIR emailed to A.F. the spreadsheet containing the usernames, encrypted passwords, and decrypted passwords of former Symplicity clients, including those of "University No. 3."

23. On or about August 15, 2011, defendant ALOK KUMAR DHIR emailed to A.F. the usernames and decrypted passwords for employees of former client, "University No. 1."

24. On or about August 17, 2011, A.F. logged into the Maxient server using the login credentials of "Employee C," an employee at Symplicity's former client "University No. 1." A.F. also attempted to login using the username and password for "Employee A," also an employee of Symplicity's former client "University No. 1."

25. A few hours after A.F. accessed Maxient's systems without authorization on or about August 17, 2011, M.K. sent an email containing ideas and talking points for how to distinguish the Symplicity SCRM product from Maxient's.

26. On or about October 27, 2011, defendant ALOK KUMAR DHIR used a security reconnaissance tool called Skipfish to identify vulnerabilities in Maxient's computer systems.

27. The statement of facts includes those facts necessary to support the defendant's guilty plea. It does not include each and every fact known to the defendant or to the government and it is not intended to be a full enumeration of all of the facts surrounding the defendant's cases.